

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

DOMINIC MAYHALL, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

AMAZON WEB SERVICES INC., *et al.*,

Defendants.

Case No. C21-1473-TL-MLP

REPORT AND RECOMMENDATION

I. INTRODUCTION

Before the Court is Defendants Amazon Web Services Inc. (“AWS”) and Amazon.com Inc.’s (collectively, “Amazon” or “Defendants”) Motion to Dismiss First Amended Complaint. (Defs.’ Mot. (dkt. ## 77, 78).) Plaintiff Ann Mayhall initially filed this action on October 29, 2021, on behalf of her minor child D.M., alleging class-action claims for: (1) violations of Illinois’s Biometric Information Privacy Act (“BIPA”), 740 ILCS 14/15; and (2) unjust enrichment. (Compl. (dkt. # 1).) Plaintiff’s claims generally arose from Amazon’s provision of cloud computing services to Take-Two Interactive (“Take Two”) and its subsidiary 2K Games for their NBA 2K video game series, which Plaintiff alleges collects and stores users’ biometric data on Amazon servers. (Compl. at ¶¶ 8-21, 166-247.)

1 On January 7, 2021, Amazon filed a motion to dismiss Plaintiff's Complaint. (Dkt. # 18.)
2 On May 24, 2022, this Court issued a Report and Recommendation (the "R&R") that
3 Defendants' motion to dismiss should be denied. (R&R (dkt. # 31).) The Honorable Tana Lin
4 issued an Order adopting the R&R and denying Amazon's motion to dismiss on March 31, 2023.
5 (Dkt. # 49.)

6 Plaintiff Dominic Mayhall ("Plaintiff") filed his First Amended Complaint (the "FAC")
7 on February 16, 2024. (Dkt. ## 72, 73.) The FAC replaces Ann Mayhall with Dominic Mayhall,
8 who is now an adult. (*Id.*) The FAC similarly alleges class-action claims for violations of BIPA
9 stemming from Amazon's alleged collection, dissemination, and storage of users' biometric data,
10 but omits the previously asserted claims for BIPA § 15(c) and unjust enrichment. (*Id.* at ¶¶ 7-28.)
11 Defendants again moved to dismiss on March 15, 2024 (Defs.' Mot. (dkt. ## 77, 78)), to which
12 Plaintiff filed a Response (dkt. ## 80, 81), and Defendants filed a Reply (dkt. ## 83, 84). The
13 Court heard oral argument from the parties on May 28, 2024. (Dkt. # 86.)

14 Having considered the parties' submissions, oral argument, the balance of the record, and
15 the governing law, the Court recommends that Defendants' Motion (dkt. ## 77, 78) be DENIED,
16 as further explained below.

17 II. BACKGROUND

18 Take-Two, and its subsidiary 2K Games, annually publish NBA 2K, a basketball video
19 game. (FAC at ¶ 8.) For online services related to the NBA 2K games, Take-Two employs
20 Amazon's cloud-computing, storage, and delivery services. (*Id.* at ¶ 9.) Plaintiff alleges that
21 AWS and Amazon.com Inc. have shared facilities and infrastructure, such that AWS enters into
22 contractual relationships with video game companies for its web services and then leverages
23 Amazon.com Inc. facilities and infrastructure to provide such services. (*Id.* at ¶¶ 63-68.)

1 Specifically, Plaintiff alleges that Take-Two uses “Amazon CloudFront,” which is a content
2 storage and delivery network that speeds up content delivery by distributing and storing content
3 at “regional” and “edge” data center locations. (*Id.* at ¶¶ 51-62, 69-74.)

4 In addition to publishing NBA 2K, Take-Two also publishes a companion app (the
5 “App”) for mobile devices that, *inter alia*, allows users to upload images of their face to assist in
6 making customized players that resemble the user. (FAC at ¶¶ 11-12.) To create a customized
7 player in this fashion, the user is required to log into the App and take 13 different photos of their
8 face. (*Id.* at ¶ 13.) The App uploads the photos to a Take-Two server. (*Id.* at ¶ 14.) The user then
9 logs into their gaming platform and selects an option when creating a customized player to use
10 their “Head Scan Data.” (*Id.* at ¶¶ 102-06.) Once selected, the game retrieves the photos from
11 Take-Two’s server and constructs a 3D model of the user’s face (the “face geometry”). (*Id.* at
12 ¶¶ 14-23, 107-10.)

13 According to Defendants’ Motion, this allegation is a key change from Plaintiff’s initial
14 Complaint, which alleged that Take-Two’s App used computing power from Amazon’s servers
15 to construct a 3D model of the user’s face geometry. (*See* Compl. at ¶¶ 16, 105-06.) The FAC no
16 longer alleges Amazon’s involvement in this process—extraction of users’ face geometry is
17 conducted by Take-Two. (*Compare id.*, with FAC at ¶¶ 16, 107.)

18 Once the face geometry is created, Plaintiff alleges that Defendants obtain the face
19 geometry, transmit it through Amazon regional and edge server locations, and deliver it to the
20 user’s online multiplayer game sessions. (FAC at ¶¶ 132-36.) Plaintiff alleges that the
21 transmitted face geometry constitutes a “biometric identifier” that Amazon stores at each
22 regional and edge server location through which it is transmitted. (*Id.* at ¶¶ 131, 144-46.)
23 Plaintiff further alleges that the process of delivering, storing, and transmitting the biometric data

1 through the server locations is repeated each time the user plays an online game with their
2 customized player. (*Id.* at ¶¶ 149-50.)

3 Per his complaint, Plaintiff created a customized player in the NBA 2K21 video game
4 while located in Illinois when he was a minor in early 2021. (FAC at ¶¶ 186-89.) To create his
5 custom player, Plaintiff took multiple pictures of his face with his cellphone and uploaded them
6 via the App. (*Id.* at ¶¶ 189-91.) Plaintiff then logged into his Xbox One to create a custom player,
7 where Plaintiff's photos were used to create his face geometry. (*Id.* at ¶¶ 190-92.)

8 Once his face geometry was created, Plaintiff alleges that Amazon transmitted it via
9 CloudFront through its regional and edge systems and delivered it to Plaintiff's Xbox One at his
10 home in Illinois. (FAC at ¶¶ 193-98.) Plaintiff alleges that Amazon stored his face geometry at
11 each regional and edge location through which it passed. (*Id.* at ¶ 195.) Accordingly, every time
12 he played NBA 2K21 with his customized player, Plaintiff alleges that Amazon obtained,
13 disseminated, and stored his biometric information. (*Id.* at ¶ 196.) Plaintiff further alleges that
14 Defendants knew they were collecting biometric data from Illinois citizens, including children, in
15 violation of Illinois state law. (*Id.* at ¶¶ 173, 178-79.)

16 III. DISCUSSION

17 Here, the Court should deny Defendants' Motion because Plaintiff's FAC plausibly
18 alleges facts for Plaintiff's §§ 15(a), (b), and (d) claims. Specifically, the Court should find: (1)
19 Plaintiff's §§ 15(a) and (d) claims sufficiently plead that Defendants were in possession of his
20 biometric data; (2) Plaintiff's § 15(b) claim sufficiently pleads that Defendants took an "active
21 step" to obtain his biometric data; and (3) the Communications Decency Act ("CDA") does not
22 preclude the FAC because Plaintiff's claims do not treat Defendants' conduct as publishing.
23

1 **A. Rule 12(b)(6) Legal Standard**

2 When considering a motion to dismiss under Rule 12(b)(6), the court construes the
3 complaint in the light most favorable to the nonmoving party. *Livid Holdings Ltd. v. Salomon*
4 *Smith Barney, Inc.*, 416 F.3d 940, 946 (9th Cir. 2005). The court must accept all well-pleaded
5 facts as true and draw all reasonable inferences in favor of the plaintiff. *Wylar Summit P'ship v.*
6 *Turner Broad. Sys., Inc.*, 135 F.3d 658, 661 (9th Cir. 1998). The court, however, is not required
7 "to accept as true allegations that are merely conclusory, unwarranted deductions of fact, or
8 unreasonable inferences." *Spewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001).

9 "To survive a motion to dismiss, a complaint must contain sufficient factual matter,
10 accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556
11 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim
12 has facial plausibility when the plaintiff pleads factual content that allows the court to draw the
13 reasonable inference that the defendant is liable for the misconduct alleged." *Id.* at 677-78. "A
14 pleading that offers 'labels and conclusions' or 'a formulaic recitation of the elements of a cause
15 of action will not do.' . . . Nor does a complaint suffice if it tenders 'naked assertion[s]' devoid
16 of 'further factual enhancement.'" *Id.* at 678 (quoting *Twombly*, 550 U.S. at 555, 557). Dismissal
17 under Rule 12(b)(6) can be based on the lack of a cognizable legal theory or the absence of
18 sufficient facts alleged under a cognizable legal theory. *Balistreri v. Pacifica Police Dep't*, 901
19 F.2d 696, 699 (9th Cir. 1990).

20 **B. Extrinsic Evidence**

21 In deciding whether to dismiss a complaint for failing to state a claim, the Court is
22 generally bound by the facts and allegations contained within the four corners of the complaint.
23 *See Shaver v. Operating Eng'rs Loc. 428 Pension Tr. Fund*, 332 F.3d 1198, 1201 (9th Cir. 2003).

1 When the complaint is accompanied by attached documents, such documents are deemed part of
2 the complaint and may be considered in evaluating the merits of a motion to dismiss. *Cothron v.*
3 *White Castle System, Inc.*, 467 F. Supp. 3d 604, 610 (N.D. Ill. 2020); *Figueroa v. Kronos Inc.*,
4 454 F. Supp. 3d 772, 778 (N.D. Ill. 2020).

5 Additionally, the Court may consider “materials incorporated into the complaint by
6 reference and matters of judicial notice.” *New Mexico State Inv. Council v. Ernst & Young LLP*,
7 641 F.3d 1089, 1094 (9th Cir. 2011). “Incorporation by reference” allows for consideration of
8 documents “whose contents are alleged in a complaint and whose authenticity no party
9 questions, but which are not physically attached to the [plaintiff’s] pleading.” *Knievel v. ESPN*,
10 393 F.3d 1068, 1076 (9th Cir. 2005) (internal quotations omitted). Documents may be
11 incorporated by reference “if the plaintiff refers extensively to the document or the document
12 forms the basis of the plaintiff’s claim.” *United States v. Ritchie*, 342 F.3d 903, 908-09 (9th Cir.
13 2003). Judicial notice may be taken of facts that are not subject to reasonable dispute because
14 they are generally known or “capable of accurate and ready determination by resort to sources
15 whose accuracy cannot be reasonably questioned.” *Id.* at 908-09; *see* Fed. R. Evid. 201(b).

16 Defendants ask the Court to consider extrinsic evidence of: (1) AWS’s Data Privacy FAQ
17 and Customer Agreement; and (2) Erick Boenisch’s 2023 declaration in its entirety. (Defs.’ Mot.
18 at 6, 11-13, Exs. B-D.) Defendants’ first request for judicial notice is nearly identical to that
19 made in its motion to dismiss the initial Complaint, and this Court previously considered
20 extrinsic evidence of Amazon’s agreements and policies. (R&R at 7-10.) Here, the Court
21 similarly finds that it may take judicial notice of AWS’s Data Privacy FAQ and Customer
22 Agreement. *See, e.g., Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1061 (N.D. Cal. 2021)
23 (taking judicial notice of Google’s Terms of Service and Privacy Policy).

1 Defendants also request that the Court consider the entirety of a 2023 declaration by Mr.
2 Boenisch that was cited once in the FAC because, they argue, its single reference incorporates
3 the entire declaration. (Defs.’ Mot. at 6, Ex. B.) Plaintiff opposes Defendants’ request, arguing
4 that Mr. Boenisch’s 2023 declaration is not sufficiently relied upon to justify incorporation into
5 the FAC. (Resp. at 6.) Even if the declaration were incorporated, Plaintiff argues that it would be
6 improper to assume the testimony’s truth, especially since Mr. Boenisch’s 2023 declaration is
7 only cited to show that witness’s inconsistent testimony. (*Id.* at 6-7.)

8 The FAC cites Mr. Boenisch’s 2023 declaration briefly in one footnote (*see* FAC at ¶ 23
9 n.1), not extensively. *See Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1003 (9th Cir.
10 2018) (“For ‘extensively’ to mean anything . . . it should, ordinarily at least, mean more than
11 once.”). Nor does the 2023 declaration form the basis of Plaintiff’s FAC—instead Plaintiff cites
12 the document to show Mr. Boenisch has previously given conflicting testimony, not to assert that
13 the testimony in the 2023 declaration is true. (*See* FAC at ¶ 23 n.1; Resp. at 6.) Even if the
14 entirety of Mr. Boenisch’s 2023 declaration were considered, “it is improper to assume the truth
15 of an incorporated document if such assumptions only serve to dispute facts stated in a well-
16 pleaded complaint.” *See Khoja*, 899 F.3d at 1003. Accordingly, the Court declines to incorporate
17 Mr. Boenisch’s 2023 declaration and will not consider it in evaluating Defendants’ Motion.

18 **C. Possession under BIPA §§ 15(a) and (d)**

19 Section 15(a) requires private entities “in possession of biometric identifiers or biometric
20 information” to:

21 develop a written policy, made available to the public, establishing a retention
22 schedule and guidelines for permanently destroying biometric identifiers and
23 biometric information when the initial purpose for collecting or obtaining such
identifiers or information has been satisfied or within 3 years of the individual’s
last interaction with the private entity, whichever occurs first. . . .

1 740 ILCS 14/15(a).

2 Section 15(d) further provides any private entity “in possession of a biometric identifier
3 or biometric information” is not permitted to “disclose, redisclose, or otherwise disseminate a
4 person’s . . . biometric identifier or biometric information” unless, in relevant part, the subject of
5 the biometric identifier or information “consents to the disclosure or redisclosure.” 740 ILCS
6 14/15(d).

7 While §§ 15(a) and (d) both regulate “possession” of biometric information, BIPA does
8 not define “possession.” *See* 740 ILCS 14/10. The Illinois Supreme Court has held possession
9 “occurs when a person has or takes control of the subject property or holds the property at his or
10 her disposal.” *People v. Ward*, 830 N.E. 2d 556, 560 (Ill. 2005). This Court and others have
11 adopted this definition when analyzing BIPA claims. *See Mayhall, et al., v. Amazon Web Servs.*
12 *Inc.*, 2022 WL 2718091, at *6 (W.D. Wash. May 24, 2022) (collecting cases), *report and*
13 *recommendation adopted*, 2023 WL 2728292 (W.D. Wash. Mar. 31, 2023).

14 As such, allegations demonstrating that the defendant in any way controlled, accessed,
15 received, or exerted dominion over the biometric data are typically required to show possession.
16 *See Naughton v. Amazon.com, Inc.*, 2022 WL 19324, at *3 (N.D. Ill. Jan. 3, 2022) (“[Plaintiff]
17 also specifically asserts that Amazon stores his biometric data in a database. This plainly satisfies
18 the ‘possession’ requirement at the pleadings stage.”); *cf. Jacobs v. Hanwha Techwin Am., Inc.*,
19 2021 WL 3172967, at *3 (N.D. Ill. July 27, 2021) (dismissing § 15(a) claim where the plaintiff
20 “does not provide any factual allegations that plausibly establish that defendant exercised control
21 over plaintiff’s data or otherwise held plaintiff’s data at its disposal”).

22 Defendants’ primary contention is that the FAC no longer establishes Amazon had
23 “possession” of Plaintiff’s biometric information because the FAC omitted an allegation from the

1 initial Complaint that Take-Two used Amazon’s computing power to extract Plaintiff’s face
2 geometry. (Defs.’ Mot. at 9.) Without this allegation, Amazon argues that it was acting solely as
3 a passive cloud storage service that exerted no control or dominion over Plaintiff’s biometric
4 information. (*Id.* at 9-11.) Plaintiff counters that possession is sufficiently alleged because
5 Amazon received his biometric data from Take-Two, repeatedly transmitted his data to multiple
6 third-party gaming platforms, and stored his data on numerous edge and regional servers. (Resp.
7 at 8-9.) These actions would be impossible without Amazon’s possession of his data. (*Id.* at 15.)

8 At this stage, the Court must accept the facts as pleaded in the FAC. While Defendants
9 assert that they had no ability to access users’ biometric data and were unaware of their receipt of
10 such information, the Court must construe the FAC’s factual allegations as true and draw
11 reasonable inferences in Plaintiff’s favor. *See Wyler Summit*, 135 F.3d at 661. The FAC alleges
12 that Defendants knowingly obtained users’ face geometry data from Take-Two and that it
13 remains in their control as they disseminate and store it on their servers. (FAC at ¶¶ 135-51,
14 173-79.) Thus, Plaintiff has at least plausibly alleged possession of biometric data, even without
15 the previously asserted allegation that Amazon extracted Plaintiff’s face geometry.

16 Nor do Defendants’ citations to its customer agreements and policies negate the FAC’s
17 allegations. As this Court previously noted, these agreements and policies show that Amazon
18 maintains some form of possession of its server data since Amazon can access and/or control
19 customer content under at least some terms of those very agreements and policies. *See Clark v.*
20 *Microsoft Corp.*, 2023 WL 5348760, at *4 (N.D. Ill. Aug. 21, 2023) (“While data storage alone
21 may be insufficient, storage of data together with the ability to control access to that data
22 adequately pleads possession.”). Again, exclusive ownership or control of the biometric data is
23 not required to show possession under §§ 15(a) and (d). *See Ward*, 215 Ill. 2d 317, 325 (rejecting

argument that “possession” requires exclusive control). Ultimately, there are still issues of fact as to what possession and/or control Amazon has over the data stored on its servers that cannot be decided at the pleading stage. Therefore, Plaintiff’s §§ 15(a) and (d) claim should not be dismissed.

D. “Active Step” under BIPA § 15(b)

Section 15(b) requires private entities that “collect, capture, purchase, receive through trade, or otherwise obtain a person’s . . . biometric identifier or biometric information” to first: (1) inform the person of that collection “in writing”; (2) inform the person “in writing of the specific purpose and length of term” regarding the collection; and (3) obtain a “written release” from the person. 740 ILCS 14/15(b).

Unlike §§ 15(a) and (d)—which apply to “possession of” biometric data—§ 15(b) applies to entities that “collect, capture, purchase, receive through trade, or otherwise obtain” biometric data. *See* 740 ILCS 14/15(a)-(d). The catch-all phrase “otherwise obtain” is not defined by BIPA.¹ *See* 740 ILCS 14/10. Courts interpreting the meaning of “otherwise obtain” have held that possession alone is not enough to subject a private entity to § 15(b). *See Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 966 (N.D. Ill. 2020) (the argument that § 15(b) requires more than mere possession “finds ample support in the case law”). Thus, this Court and others have concluded that for § 15(b) to apply the defendant must take active steps to collect, capture, or otherwise obtain the plaintiff’s biometric information. *See Mayhall*, 2022 WL 2718091, at *10 (collecting cases).

¹ “Obtain” is defined as “[t]o come into the possession of,” or “to get, acquire, or secure.” *Vance v. Amazon.com Inc.*, 525 F. Supp. 3d 1301, 1312 (W.D. Wash. 2021) (citing *Obtain*, Oxford English Dictionary). “Otherwise” means “[i]n a different manner; in another way, or in other ways.” *Id.* (citing Black’s Law Dictionary 1101 (6th ed. 1990); *Otherwise*, Oxford English Dictionary).

1 Defendants primarily contend that Plaintiff fails to allege Amazon took an “active step”
2 to collect, capture, purchase, or otherwise obtain biometric data since the FAC omits allegations
3 that Amazon used its computing power to extract Plaintiff’s face geometry. (Defs.’ Mot. at
4 13-15.) Plaintiff first asserts that § 15(b) does not require an “active step.” (Resp. 12-14.) But
5 even if an “active step” is required, Plaintiff argues that Defendants’ collection, dissemination,
6 and continuing storage of his face geometry constitute affirmative actions to “otherwise obtain”
7 his biometric data and meet § 15(b)’s requirements. (Resp. at 14-16.)

8 Plaintiff has sufficiently alleged that Amazon “otherwise obtained” biometric data. (*See*
9 FAC at ¶¶ 135-51.) First, contrary to Amazon’s argument, Plaintiff’s allegations establish more
10 than passive possession. *See Rivera v. Amazon Web Servs., Inc.*, 2023 WL 4761481, at *5 (W.D.
11 Wash. July 26, 2023) (collection allegation sufficient where “Amazon continues to act as the
12 ‘cloud-service provider’ . . . and thus is able to ‘access’ and ‘extract’ biometric data”); *Vance v.*
13 *Amazon.com Inc.*, 525 F. Supp. 3d 1301, 1312-13 (W.D. Wash. 2021) (finding plaintiffs
14 sufficiently alleged Amazon received biometric data “in some other way—namely by applying
15 for and downloading the data set from IBM”); *Figueroa*, 454 F. Supp. 3d at 784 (“[T]o have
16 [stored or used] the data, [the defendant] necessarily first had to ‘obtain’ the data.”). Specifically,
17 the FAC alleges that Amazon obtained and subsequently stored the biometric data on its regional
18 and edge servers. (*See* FAC at ¶¶ 139-41, 144-49.) Next, Plaintiff alleges that Amazon
19 disseminated the face geometry to third-party gaming platforms every time Plaintiff played an
20 online multiplayer game and kept Plaintiff’s biometric data even after the games ended. (*See id.*
21 at ¶¶ 140-50; 193-96.) To do any of these things, Amazon “necessarily first had to ‘obtain’ the
22 data.” *Figueroa*, 454 F. Supp. 3d at 784. Therefore, Plaintiff’s § 15(b) claim should not be
23 dismissed.

1 **E. The Communications Decency Act**

2 Finally, Defendants argue that Plaintiff’s claims are precluded by § 230(c)(1) of the CDA
3 because Amazon is an internet computer service that allegedly “published Take-Two’s data to
4 online NBA2K opponents.” (Reply at 9.) “[S]ubsection (c)(1) only protects from liability (1) a
5 provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a
6 state law cause of action, as a publisher or speaker (3) of information provided by another
7 information content provider.” *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100–01 (9th Cir. 2009),
8 *as amended* (Sept. 28, 2009); *see* 47 U.S.C. § 230. “[P]ublication involves reviewing, editing,
9 and deciding whether to publish or to withdraw from publication third-party content.” *Barnes*,
10 570 F.3d at 1102. “[C]ourts must ask whether the duty that the plaintiff alleges the defendant
11 violated derives from the defendant’s status or conduct as a ‘publisher or speaker.’” *Id.*

12 The CDA is inapplicable because Plaintiff’s BIPA claims do not treat Amazon’s conduct
13 as publishing. Rather, BIPA imposes legally distinct duties to make certain disclosures and
14 obtain consent before obtaining or using biometric information. These duties do not derive from
15 or even require publishing—they arise from Defendants’ alleged possession, use, and/or
16 dissemination of biometric data without notice or consent. *See, e.g., In re Soc. Media Adolescent*
17 *Addiction/Pers. Inj. Prod. Liab. Litig.*, 2023 WL 7524912, at *17 (N.D. Cal. Nov. 14, 2023)
18 (“The claim alleges defendants failed to provide required notice and obtain parental consent
19 before collecting certain information from children. That in no way impacts their role as
20 publishers of third-party content.”). Indeed, Defendants cite no cases where courts apply the
21 CDA to duties imposed by BIPA. (*See* Defs.’ Mot.; Reply; *see also* Resp. at 19 n.10.) Likewise,
22 § 230 of the CDA provides no immunity here.
23

1 Defendants' policy arguments—that requiring Amazon to obtain consent from or make
2 disclosures to “total strangers” would lead to “absurd” outcomes—are likewise unavailing. (*See*
3 Defs.’ Mot. at 18-19.) The Court in *Rivera v. Amazon Web Services, Inc.* considered and rejected
4 a similar argument from AWS, and instead found that AWS was connected to users through its
5 customer. 2023 WL 4761481, at *6. “[I]t is therefore not inconceivable that Amazon could
6 notify [users] and obtain their consent during the image upload process.” *See id.* Likewise,
7 Defendants are not “total strangers” to Plaintiff and similarly situated users because, as Plaintiff
8 alleges, they are connected through Amazon’s customer Take-Two. *See id.* Furthermore,
9 Defendants fail to explain why they should be excluded from BIPA liability simply because they
10 did not obtain biometric information directly from users. “Whether that biometric information
11 comes from an individual or is part of a large dataset, there is nothing absurd about requiring any
12 entity that obtains such information to comply with the safeguards that the Illinois legislature
13 deemed necessary.” *Vance*, 525 F. Supp. 3d at 1313. Accordingly, this Court recommends that
14 Defendants’ Motion be denied.

15 **F. Motions to Seal**

16 The parties moved to file the FAC, Motion, Response, and Reply under seal to protect
17 confidential third-party information pursuant to the Stipulated Protective Order (dkt. # 37). The
18 Court granted Plaintiff’s motion to file the FAC under seal (dkt. # 62) on February 8, 2024. (Dkt.
19 # 71.) The parties’ motions to seal Defendants’ Motion (dkt. # 76), Response (dkt. # 79), and
20 Reply (dkt. # 82) are still pending.

21 The parties argue that filing under seal is necessary to protect confidential materials from
22 Defendants and non-party Take-Two. (*See, e.g.*, dkt. # 76 at 1-2.) Take-Two’s materials include
23 arbitration-related documents that were produced in discovery related to a separate matter and

1 are subject to this case’s Protective Order. (*Id.*) Take-Two has designated these materials as
2 confidential because they contain “commercially-sensitive information relating to the
3 development, creation, and operation of its NBA 2K videogame as well as its proprietary
4 MyPLAYER avatar that its players use.” (*Id.*) Similarly, Defendants seek to maintain
5 confidentiality of payment information relating to its contracts and invoices for services. (Dkt.
6 # 79 at 1-2.)

7 The Court has previously granted the parties’ request to file these materials under seal
8 (dkt. # 71), and this Court likewise finds compelling reasons for the parties to file this
9 confidential information under seal. *See Apple, Inc. v. Samsung, Elecs. Co., Ltd.*, 727 F.3d 1214,
10 1221 (9th Cir. 2013) (“One factor that weighs in favor of sealing documents is when the release
11 of the documents will cause competitive harm to a business.”). Accordingly, the Court GRANTS
12 the parties’ motions to seal Defendants’ Motion (dkt. # 76), Plaintiff’s Response (dkt. # 79), and
13 Defendants’ Reply (dkt. # 82).

14 IV. CONCLUSION

15 For the forgoing reasons, the Court recommends that Defendants’ Motion (dkt. ## 77, 78)
16 be DENIED. A proposed Order accompanies this Report and Recommendation.

17 Objections to this Report and Recommendation, if any, should be filed with the Clerk and
18 served upon all parties to this suit not later than **fourteen (14) days** from the date on which this
19 Report and Recommendation is signed. Failure to file objections within the specified time may
20 affect your right to appeal. Objections should be noted for consideration on the District Judge’s
21 motions calendar **fourteen (14) days** from the date they are filed. Responses to objections may
22 be filed by **the day before the noting date**. If no timely objections are filed, the matter will be
23 ready for consideration by the District Judge on **June 13, 2024**.

1 The Clerk is directed to send copies of this Report and Recommendation to the parties
2 and to the Honorable Tana Lin.

3 Dated this 29th day of May, 2024.

4
5 

6 MICHELLE L. PETERSON
7 United States Magistrate Judge
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23